

definitiva de dominio público. Que no puede invocarse como fundamento legal de la revocación pretendida la Resolución mencionada, ya que nada tiene que ver con este supuesto de hecho. 5. Que no es el lugar adecuado para abordar la cuestión de nulidad del artículo 35 del Reglamento de Costas. Que dicho artículo impide practicar segundas y ulteriores inscripciones sobre la registral 13.851, puesto que la anotación letra B publica que la misma forma parte del dominio público marítimo-terrestre. 6. Que en este supuesto, practicada la anotación de dominio público, se notificó esta circunstancia a la titular registral a fin de que la misma, si así convenía a su derecho, pudiera interponer la correspondiente demanda contra el acto administrativo afectante a su titularidad registral y solicitar su anotación en el Registro de la Propiedad dentro del año siguiente a dicha notificación, para que el Registro publicase la existencia del eventual litigio afectante a la delimitación demanial sobre la finca de su titularidad con los efectos inherentes a dicha anotación de demanda. 7. Que los artículos 4 y 5 de la Ley de Costas suponen una excepción a los principios de legitimación y fe pública registral. 8. Que hay que considerar lo que argumenta el fundamento de derecho sexto de la Resolución de 15 de marzo de 1993. Que como fundamentos de derecho hay que señalar los artículos 18 y 42 de la Ley Hipotecaria, 9 y 15 de la Ley de Costas y 31 y siguientes del Reglamento de Costas y las Resoluciones de 16 de diciembre de 1991, 8 de enero y 15 de marzo de 1993, 16 de julio de 1998 y 14 de enero de 2000.

Fundamentos de Derecho

Vistos los artículos 1 y 71 de la Ley Hipotecaria, 11, 13.1 y disposición transitoria 2.ª, 3, de la Ley de Costas y 29.2.a) del Reglamento de Costas.

1. Se debate en el presente recurso si la existencia sobre determinada finca de una anotación preventiva de las previstas en el artículo 29.2.a) del Reglamento de Costas, relativa a sentencia de aprobación del deslinde de la zona marítimo-terrestre, impide la inscripción de la venta de dicha finca efectuada por quién aparece como titular registral de la misma antes de dicho deslinde, habida cuenta que, cuando se presenta a inscripción el documento calificado ha transcurrido con creces el plazo del año contado desde la notificación por el Registrador de aquella anotación, previsto en el apartado c) del citado artículo.

2. Ciertamente, la anotación cuestionada recoge un pronunciamiento dominical incompatible con el del otorgante del documento calificado (cfr. artículos 11 y siguientes de la Ley de Costas, en especial, artículo 13-1 y disposición transitoria 2.ª, 3). Ahora bien: Si se tiene en cuenta que se trata de un pronunciamiento recaído en trámite meramente administrativo que contradice asientos registrales que están bajo la salvaguarda de los tribunales (cfr. artículo 1 de la Ley Hipotecaria), y que invierte, a favor de la Administración, la carga de la iniciativa procesal dirigida al mantenimiento de tales asientos, (por cuya razón, el artículo 29 del Reglamento de Costas, sobre la base de la delegación legislativa contenida en el artículo 13 de la Ley de Costas, establece esta fase intermedia o provisional en la eficacia rectificadora registral de la aprobación del deslinde); y si se considera que los derechos objeto de anotación son, como regla, enajenables, sin perjuicio del derecho de la persona a cuyo favor se practicó la anotación (cfr. artículo 71 de la Ley Hipotecaria), habrá de concluirse en la inscribibilidad de la enajenación calificada, sin perjuicio, claro está, de la prevalencia de la anotación preexistente, que comportará la sujeción de aquella inscripción a las consecuencias inherentes a la definitiva rectificación registral que tal anotación anuncia.

Esta Dirección General ha acordado estimar el recurso y revocar la nota impugnada.

Contra esta Resolución, los legalmente legitimados, pueden recurrir mediante demanda ante el Juzgado de lo Civil de la capital de la provincia del lugar donde radica el inmueble en el plazo de dos meses desde su notificación, siendo de aplicación las normas del juicio verbal, todo ello conforme a lo establecido en los artículos 325 y 328 de la Ley Hipotecaria.

Madrid, 10 de junio de 2002.—La Directora general, Ana López-Monís Gallego.

Sr. Registrador de la Propiedad de El Puerto de Santa María.

MINISTERIO DE HACIENDA

14810 RESOLUCIÓN de 8 de julio de 2002, de la Secretaría de Estado de Presupuestos y Gastos, para el control de accesos a las bases de datos de la Secretaría de Estado.

El Real Decreto 1330/2000, de 7 de julio, de estructura orgánica básica del Ministerio de Hacienda, establece en su artículo 9, apartado 1, h), que la Intervención General de la Administración del Estado es el órgano encargado de la planificación, diseño y ejecución de la política informática de la Secretaría de Estado de Presupuestos y Gastos, el soporte informática de las actividades y el asesoramiento, coordinación e instrumentación de los proyectos informáticos de sus órganos.

Los sistemas de información y las bases de datos que en ellos se soportan constituyen un elemento básico para la gestión encomendada a la Secretaría de Estado de Presupuestos y Gastos, por lo que deben ser objeto de una especial protección a fin de que cumplan los requisitos de disponibilidad, integridad y confidencialidad precisos.

En consecuencia, las funciones que puedan realizarse en los sistemas de información han de tratarse de forma que faciliten las elaboraciones específicas y concretas de gestión para las que han sido diseñadas, al mismo tiempo que quedan encuadradas en el marco general del control de accesos a la información que salvaguarde la integridad y la confidencialidad de los datos contenidos en los sistemas.

Por todo ello, y de conformidad con lo dispuesto en el artículo 45.3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se hace preciso establecer los criterios de regulación de un sistema de control de accesos a los sistemas de información de la Secretaría de Estado de Presupuestos y Gastos que tenga en cuenta las orientaciones antes indicadas.

En su virtud, a propuesta de la Intervención General de la Administración del Estado, he tenido a bien disponer:

Primero. *Ámbito de aplicación.*—La presente Resolución será de aplicación a toda la información contenida en cualquiera de los ficheros, organizados por un sistema gestor de bases de datos o en cualquier otra forma, que fueran objeto de tratamiento a través de los sistemas de información y aplicaciones informáticas de la Secretaría de Estado de Presupuestos y Gastos, en adelante bases de datos de la Secretaría de Estado de Presupuestos y Gastos, regulando el acceso a dicha información con arreglo a las normas de la Ley Orgánica 15/1999, de 13 de diciembre, del Real Decreto 994/1999, de 11 de junio, y de la Ley General Presupuestaria.

No se consideran dentro del ámbito de aplicación de esta Resolución las bases de datos accesibles a través del sitio web Intranet e Internet de la Secretaría de Estado de Presupuestos y Gastos, cuando tengan carácter abierto a nivel corporativo de la propia Secretaría de Estado, así como las bases de datos generadas a través de las herramientas corporativas ofimáticas o análogas a disposición del usuario.

A efectos de esta Resolución, los sistemas de información de la Secretaría de Estado de Presupuestos y Gastos están constituidos por el conjunto de datos, documentación, procedimientos y tratamientos informáticos, así como por las bases de datos, las redes de comunicaciones y los sistemas de interconexión, los sistemas de control de accesos, y los ordenadores, periféricos y terminales instalados en los Servicios centrales y Organizaciones delegadas y territoriales de la Secretaría de Estado de Presupuestos y Gastos.

En el contexto de esta Resolución se consideran Servicios centrales de la Secretaría de Estado de Presupuestos y Gastos a los centros directivos de la misma, y organizaciones delegadas y territoriales a las Unidades que tengan ese carácter y que dependan de los centros directivos de la Secretaría de Estado de Presupuestos y Gastos.

Igualmente, a efectos de esta Resolución, se denominará «servicios de Informática Presupuestaria» al área de la Intervención General de la Administración del Estado encargada del desarrollo y ejecución de las actividades informáticas de la Secretaría de Estado de Presupuestos y Gastos. Asimismo, se utilizará el término «red de Informática Presupuestaria» para hacer referencia a la red corporativa de área extensa (WAN) de la Secretaría de Estado de Presupuestos y Gastos.

Del mismo modo, cuando en esta Resolución se hace uso de la expresión «acceso a la red» se está refiriendo realmente al acceso a los servicios de red.

Segundo. *Clasificación de los sistemas de información de la Secretaría de Estado de Presupuestos y Gastos.*—Según la residencia de las bases de datos, los sistemas de información y aplicaciones informáticas de la Secretaría de Estado de Presupuestos y Gastos se clasificarán como:

- a) Centrales, si las bases de datos se ubican en los servicios de Informática Presupuestaria.
- b) Departamentales, si se ubican en los centros directivos de la Secretaría de Estado de Presupuestos y Gastos o en organizaciones delegadas y territoriales.
- c) Externos, si las bases de datos residen fuera del entorno de la Secretaría de Estado de Presupuestos y Gastos.

Tercero. *Objeto.*—El objeto de esta Resolución es establecer los criterios generales a los que debe responder la administración de la seguridad de los sistemas de información y definir el procedimiento de gestión para el acceso a los mismos en el ámbito de aplicación establecido en el apartado anterior, tanto desde la propia red corporativa de Informática Presupuestaria como desde cualquier otro organismo público con acceso autorizado. Esta seguridad cabe entenderla, a efectos de esta Resolución, en su acepción de control de los accesos a la red y a las bases de datos para garantizar la disponibilidad, integridad y confidencialidad de la información.

Estas instrucciones se aplicarán a todo el personal de la Secretaría de Estado de Presupuestos y Gastos y a aquellas personas que no perteneciendo a ésta dispongan de acceso a sus bases de datos.

Cuarto. *Agentes para la administración de la seguridad.*—La gestión de la seguridad de las bases de datos de la Secretaría de Estado de Presupuestos y Gastos requiere, además de la implicación activa de todos los usuarios de los sistemas de información, la existencia de un marco organizativo orientado a dicha gestión en el que desempeñarán un papel primordial los siguientes agentes:

- a) Comité de Coordinación de la Seguridad.
- b) Administrador corporativo de seguridad.
- c) Responsables de seguridad en los centros directivos, organizaciones delegadas o territoriales de la Secretaría de Estado de Presupuestos y Gastos, a los que en lo sucesivo esta Resolución se referirá como responsables de centro.
- d) Administradores de la seguridad de acceso a las redes departamentales de cada uno de los centros directivos, organizaciones delegadas o territoriales de la Secretaría de Estado de Presupuestos y Gastos, a los que en lo sucesivo esta Resolución se referirá como Administradores de red.
- e) Administradores de la seguridad de acceso a las bases de datos de la red de Informática Presupuestaria, a los que en lo sucesivo esta Resolución se referirá como Administradores de base de datos.

En el contexto de esta Resolución, los términos de Administrador de red y de base de datos tienen un carácter organizativo, de acuerdo con las funciones encomendadas en los apartados octavo y noveno, y no un significado informático.

Quinto. *Comité de Coordinación de la Seguridad.*—El Comité de Coordinación de la Seguridad estará formado por:

- a) El Coordinador de los servicios de Informática Presupuestaria, que actuará como Coordinador del Comité.
- b) El Subdirector general de Explotación de los servicios de Informática Presupuestaria.
- c) El Administrador corporativo de seguridad, que se establece en el apartado siguiente.
- d) Los responsables de centro, previstos en el apartado séptimo, designados por el titular de cada uno de los centros directivos de la Secretaría de Estado de Presupuestos y Gastos.
- e) Tres Interventores delegados en representación del conjunto de las Intervenciones delegadas en Ministerios y organismos autónomos, Intervenciones Regionales y Territoriales, designados por el Interventor general de la Administración del Estado.

El Comité de Coordinación de la Seguridad podrá convocar a representantes de Unidades Organizativas externas que accedan a bases de datos de la Secretaría de Estado de Presupuestos y Gastos.

A este Comité de Coordinación, que se reunirá al menos dos veces al año, le corresponderá establecer las directrices, normas y actuaciones de orden técnico que sean precisas en desarrollo de lo dispuesto en esta Resolución, dirigidas a garantizar la disponibilidad, integridad y confidencialidad de la información en la red de Informática Presupuestaria, todo ello sin perjuicio del ejercicio de las competencias decisorias por los órganos superiores o directivos del Departamento que las tengan atribuidas.

Sexto. *Administrador corporativo de seguridad.*—El Administrador corporativo de seguridad aplicará las medidas de seguridad a las bases de datos de la Secretaría de Estado de Presupuestos y Gastos de acuerdo con las directrices marcadas por el Comité de Coordinación de la Seguridad. Será designado por el Comité de Coordinación de la Seguridad a propuesta del Coordinador de Informática Presupuestaria.

El diseño, construcción, implantación y mantenimiento de las instrucciones, procedimientos y herramientas que, en aplicación de lo dispuesto en esta Resolución, se desarrollen para la administración de la seguridad de la red y de las bases de datos corresponderá a los servicios de Informática Presupuestaria bajo la iniciativa y coordinación del Administrador corporativo de seguridad, que las pondrá en conocimiento de los Responsables de los centros directivos u organizaciones delegadas o territoriales de la Secretaría de Estado de Presupuestos y Gastos, de los Administradores de red y de base de datos y, en general, las difundirá a todo el ámbito de aplicación.

Séptimo. *Responsables de centro.*—A efectos de esta Resolución se considera responsable de centro a la persona que designe el titular del centro directivo o al titular de la organización delegada o territorial de la Secretaría de Estado de Presupuestos y Gastos.

Este responsable de centro asumirá, en materia de seguridad, las funciones y obligaciones que se indican a continuación:

- a) Adoptará las medidas necesarias para el cumplimiento, en su ámbito de competencia, de las normas, instrucciones y procedimientos que, en aplicación de lo establecido en esta Resolución, se desarrollen para la administración de la red y de las bases de datos de la Secretaría de Estado de Presupuestos y Gastos.
- b) Adoptará las medidas necesarias para que el personal de su ámbito de competencia conozca las normas y procedimientos de seguridad que afecten al desarrollo de sus funciones.
- c) Designará a un Administrador único de red. No obstante, en el caso de los centros directivos, la designación del Administrador de red podrá efectuarse, si la estructura así lo aconseja, a nivel de Subdirección General o de ubicaciones administrativas diferentes.
- d) Designará a los Administradores de base de datos de su ámbito de competencia.
- e) Autorizará el acceso de usuarios a la red departamental y a las bases de datos de su centro. Asimismo, comunicará la anulación de los accesos permitidos a la red departamental y a las bases de datos de su propio centro.
- f) Solicitará el acceso de su personal a las bases de datos de la Secretaría de Estado de Presupuestos y Gastos, distintas de aquéllas residentes en su centro, que se requiera para el ejercicio de las funciones encomendadas.
- g) Designará al responsable de los ficheros de su competencia funcional, en los términos establecidos por el Real Decreto 994/1999.

En los centros directivos, las funciones d), e), f) y g) podrán ser desempeñadas por los Subdirectores Generales o asimilados, respecto a las redes, bases de datos y ámbito de personal de su respectiva competencia. Para tales funciones, y a los efectos de esta Resolución, dichos Subdirectores serán considerados como responsables de centro.

Octavo. *Administrador de red departamental.*—Cada Administrador de red será el responsable de la aplicación, en su ámbito de actuación, de la presente Resolución y de las instrucciones y procedimientos que en materia de gestión de red y del control de accesos a la misma se desarrollen. Para esta misión el Administrador de red actuará de acuerdo con las instrucciones, procedimientos y herramientas de carácter técnico que establezcan los servicios de Informática Presupuestaria.

Las funciones y obligaciones del Administrador en materia de gestión de red y control de accesos a la misma, serán:

- a) Instrumentar las solicitudes de acceso a la red de los nuevos usuarios autorizados.
- b) Realizar el mantenimiento y actualización del inventario de usuarios con acceso permitido a la red departamental.
- c) Obtener periódicamente, mediante los medios puestos a su disposición por los servicios de Informática Presupuestaria, estadística de accesos a los sistemas de información, realizados por los usuarios de la red departamental.
- d) Mantener y custodiar la información necesaria sobre la autorización y denegación del acceso de cada uno de los usuarios a la red (puesto de trabajo, responsable de la autorización y anulación de los accesos, fecha de autorización o denegación, ...).
- e) Informar de los incidentes relativos a la seguridad de control de accesos, según los procedimientos establecidos para tal fin.

Noveno. *Administrador de base de datos.*—Cada base de datos, correspondiente a un sistema de información o aplicación informática, tendrá asignado un Administrador de base de datos cuya designación corresponderá a:

a) En caso de base de datos centrales, al responsable del centro directivo al que compete la naturaleza funcional del sistema de información o aplicación informática.

Cuando el contenido de la base de datos central sea el resultado de una gestión descentralizada, el responsable del centro competente podrá designar tantos Administradores de base de datos como unidades u oficinas de gestión participen.

Cuando se trate de productos o aplicaciones informáticas de utilización general en todo el entorno de la Secretaría de Estado de Presupuestos y Gastos, sin adscripción funcional, el Administrador de base de datos será designado por el Coordinador de los servicios de Informática Presupuestaria.

b) En el caso de bases de datos departamentales, al responsable del centro directivo u organización delegada o territorial en la que residan.

c) En el caso de bases de datos externas, al Coordinador de los servicios de Informática Presupuestaria.

El Administrador de base de datos será el responsable de la aplicación de la presente Resolución y de las instrucciones y procedimientos que, en materia de control de accesos a las bases de datos, se desarrollen. Para esta misión el Administrador de base de datos actuará de acuerdo con las instrucciones, procedimientos y herramientas de carácter técnico que establezcan los servicios de Informática Presupuestaria.

Por tanto, las funciones y obligaciones del Administrador de base de datos serán:

a) Instrumentar y gestionar las altas, bajas y el mantenimiento de autorizaciones de acceso a los usuarios de las bases de datos y, en algunos casos, de las funciones permitidas (por ejemplo, asignación de perfiles de acceso).

b) Instrumentar y gestionar el acceso de los usuarios externos a las bases de datos de la red de Informática presupuestaria, previa comunicación a la Unidad de los servicios de Informática Presupuestaria designada a tal efecto.

c) Mantener y custodiar la información necesaria sobre la autorización o denegación del acceso de los usuarios a la base de datos.

d) Obtener periódicamente, mediante los medios puestos a su disposición por los servicios de informática presupuestaria, estadística de los accesos realizados por los usuarios a las bases de datos centrales y departamentales administradas por él.

Cuando se trate de bases de datos o ficheros con datos de carácter personal, a los que resulten de aplicación las medidas de seguridad de nivel alto del Real Decreto 994/1999, el Administrador de base de datos, central o departamental, obtendrá un informe mensual de los accesos y operaciones realizadas por los usuarios del sistema identificando, como mínimo, el usuario, fecha y hora en que se realizó el acceso, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

e) Informar de los incidentes relativos a la seguridad según los procedimientos establecido para tal fin.

Décimo. *Control de acceso a la red y a las bases de datos.*—El acceso a la red y los sistemas de información de la Secretaría de Estado de Presupuestos y Gastos se articulará sobre un conjunto de procedimientos integrados que se indican a continuación:

a) Todas las estaciones de trabajo de la red de informática presupuestaria, con carácter general y sin perjuicio de las excepciones que se autoricen, se configurarán de acuerdo con el procedimiento técnico de integración de sistemas de los servicios de informática presupuestaria (ISIP).

b) Todo usuario de los sistemas de información de los servicios de informática presupuestaria tendrá asignado un perfil de acceso, instrumentado sobre medios informáticos, entendiéndose como tal el catálogo de sistemas de información o aplicaciones informáticas a los que puede acceder. La asignación del perfil de acceso solamente se producirá después de haber introducido una palabra de paso de identificación personal (PIP), asociada al código identificativo del usuario lógico que accede al sistema, de forma que todo usuario autorizado a acceder a la red quede debidamente identificado y autenticado.

c) El perfil de acceso o el escritorio informático personalizado de cada usuario vendrá determinado por el conjunto de las autorizaciones de acceso otorgadas a un mismo usuario por los Administradores de bases de datos.

d) Todos los sistemas de información que se consideren críticos en materia de seguridad, o que contengan ficheros con datos de carácter personal, dispondrán de una administración que permita asignar perfiles específicos de acceso para evitar que se acceda a datos o recursos con derechos distintos de los autorizados.

Asimismo, los sistemas de información que contengan ficheros con datos de carácter personal a los que se asigne nivel de seguridad medio o alto, según lo establecido en el Real Decreto 994/1999, dispondrán de un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. Adicionalmente se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

e) La comunicación de las autorizaciones de acceso a la red y a las bases de datos efectuada por los responsables de centro con destino a los correspondientes Administradores de red y de base de datos, y, en general, las comunicaciones relativas a la administración de los accesos a la red y a las bases de datos realizadas entre los distintos agentes para la administración de la seguridad, se establecerán mediante un sistema de correo electrónico, que permita garantizar la autenticidad del origen y destino del mensaje, así como la integridad del mismo. Asimismo, los Administradores de red y base de datos enviarán una copia de los envíos y recepciones de información relativa a la administración de la seguridad, con el resto de agentes, a un buzón único, al efecto de constituir un registro histórico de control del acceso a la red y a las bases de datos de la Secretaría de Estado de Presupuestos y Gastos.

f) La integridad y actualización consistente de este registro histórico de control de accesos, así como su explotación, estarán a cargo del Administrador corporativo de seguridad.

Undécimo. *Integración de sistemas de los servicios de informática presupuestaria (ISIP).*—Con objeto de garantizar una configuración normalizada de todas las estaciones de trabajo de la red corporativa de informática presupuestaria, con carácter general y sin perjuicio de las excepciones que se autoricen, su instalación se ajustará al procedimiento técnico de integración de sistemas de los servicios de informática presupuestaria (ISIP) que garantizará:

a) El control normalizado de acceso a la red mediante la identificación personalizada, en el arranque del puesto de trabajo, a través del identificativo lógico de usuario y de la introducción de una palabra de paso personal (PIP) asociada.

b) La configuración del escritorio personalizado del puesto de trabajo, integrado por el conjunto de sistemas de información a los que el usuario del mismo puede acceder.

c) La distribución de «software» al puesto de trabajo y, en su caso, al servidor departamental.

Duodécimo. *Autorización de acceso a la red.*—El alta inicial de un nuevo usuario, para acceder a la red departamental que le corresponda, requerirá la autorización del responsable del centro directivo u organización delegada o territorial, dirigida al Administrador de la red, a quien competirá instrumentar dicha alta. La comunicación de la autorización se realizará por correo electrónico y en ella se indicará, al menos, el nombre y apellido de la persona para la que se solicita el acceso, el puesto de trabajo que ocupa y un teléfono de contacto.

Asimismo, el responsable del centro directivo u organización delegada o territorial, comunicará puntualmente al Administrador de la red, a través de correo electrónico, las revocaciones de las autorizaciones vigentes a favor del personal que deje de prestar sus servicios en el ámbito organizativo que corresponde a dicha red departamental o que, continuando prestando servicios en la Organización, no precisen disponer de acceso a la red.

Decimotercero. *Tramitación de acceso a la red.*—El Administrador de la red tramitará la solicitud de acceso a la red. Una vez efectuada el alta de usuario, el Administrador de la red comunicará al nuevo usuario su identificativo lógico y una palabra de paso de identificación personal (PIP), de carácter inicial. Esta PIP deberá ser necesariamente renovada por el usuario, generando otra distinta, al producirse el primer acceso, después de haber contabilizado un número determinado de accesos a la red y, en todo caso, transcurridos el número de días que se establezca por la Intervención General de la Administración del Estado. Asimismo el usuario podrá generar, en cualquier momento, una nueva PIP que sustituya a la anterior.

El sistema informático registrará la PIP de forma criptografiada, de tal manera que no sea posible su lectura.

Asimismo, con la información recibida del responsable del centro directivo u organización delegada o territorial, el Administrador de la red ges-

tionará, con puntualidad, las bajas de los correspondientes identificativos lógicos de usuario.

El Administrador de red será responsable del mantenimiento y actualización del inventario de usuarios con acceso permitido a la red departamental y de la custodia y almacenamiento de la información necesaria para la autorización de cada uno de ellos: Identificación de la persona y puesto de trabajo que ocupa; responsable jerárquico que concedió la autorización y fecha de la misma; responsable jerárquico que autorizó su anulación y motivo de la misma.

El Administrador de red deberá archivar, al menos durante dos años, el correo recibido, de autorización de acceso a la red, del responsable del centro directivo u organización delegada o territorial. De igual manera, deberá archivar los correos enviados de notificación de habilitación de acceso al responsable del centro directivo, organización delegada o territorial y al usuario.

El envío y recepción de información relativa a la administración de los accesos a la red, con el resto de agentes para la administración de la seguridad, y la copia de cada uno de estos intercambios de información al buzón único de seguridad, se realizarán, según establece el apartado décimo, e), mediante un sistema de correo electrónico.

Decimocuarto. *Solicitud de acceso a base de datos.*—La solicitud de acceso a una base de datos será dirigida a quien, según el apartado séptimo, corresponde la autorización de acceso, por el responsable jerárquico superior del usuario para el que se solicita el acceso, que, en el caso de servicios centrales, tendrá categoría mínima de Subdirector general o asimilado y, en el supuesto de tratarse de organizaciones delegadas o territoriales, será el máximo responsable de la organización. En esta solicitud se indicarán los usuarios, con su identificativo, para los que se propone el acceso, el sistema de información a acceder, el perfil de acceso requerido, una justificación debidamente fundamentada, la ubicación y una persona de contacto. Asimismo se indicará la fecha propuesta para el alta y la fecha de caducidad para dicho acceso.

No obstante lo anterior, cuando el usuario que requiere el acceso a la base de datos pertenezca al mismo Centro al que compete la administración funcional de la base de datos, la solicitud de acceso será dirigida directamente al correspondiente Administrador de base de datos por el responsable jerárquico superior del usuario, para el que se requerirá la misma categoría indicada en el párrafo anterior.

Decimoquinto. *Autorización y tramitación de acceso a base de datos.*—La autorización, en su caso, de la solicitud de acceso a la base de datos será dirigida por el responsable de centro al que corresponda la administración funcional de la base de datos al Administrador de base de datos. Esta comunicación se realizará por correo electrónico, sin perjuicio de la remisión adicional de la documentación constitutiva de la solicitud.

Corresponde al Administrador de base de datos la instrumentación de la autorización o denegación de acceso y su notificación al responsable jerárquico superior del usuario.

No obstante, conforme a lo señalado en el apartado anterior, cuando la solicitud se refiera a un usuario que pertenezca al mismo Centro al que compete la administración funcional de la base de datos, no será precisa la expresa autorización del responsable de centro correspondiente, actuando el Administrador de base de datos conforme a los criterios generales de autorización que establezca el responsable de centro.

Por tanto, se responsabilizará el Administrador de base de datos de la gestión del alta, baja y mantenimiento de autorizaciones de acceso al sistema de información, así como de la asignación de perfiles de acceso, cuando según el apartado siguiente haya de efectuarse, que deberán corresponderse con las necesidades concretas de gestión. Asimismo dicho Administrador procederá, a iniciativa propia, a la depuración de las autorizaciones de acceso al sistema de información, habilitando los procedimientos necesarios para disponer la caducidad de las autorizaciones de acceso cuando fuera procedente a juicio del Administrador, o cuando se dieran las circunstancias que aconsejaran tal medida, notificando dicha actuación al responsable jerárquico del usuario afectado.

El Administrador de base de datos deberá archivar, al menos durante dos años, el correo recibido, en su caso, del responsable de centro, junto con la documentación constitutiva de la solicitud, así como los correos de notificación de habilitación de acceso enviados a dicho responsable de centro, al responsable jerárquico superior del usuario y al usuario afectado.

El envío y recepción de información relativa a la administración de los accesos a la base de datos, con el resto de agentes para la administración de la seguridad, y la copia de cada uno de estos intercambios de información al buzón único de seguridad se realizarán, según establece el apartado décimo e), mediante un sistema de correo electrónico.

Decimosexto. *Acceso a sistemas de información críticos en materia de seguridad.*—En aquellos sistemas de información críticos en materia de seguridad, o que contengan ficheros con datos de carácter personal, el respectivo Administrador de base de datos podrá requerir en el formulario de solicitud, las funciones o/y el dominio de datos a los que se propone acceder por parte del usuario para el que se formula la misma.

En estos casos, el usuario autorizado accederá exclusivamente a las funciones y al dominio de datos expresamente indicados por el correspondiente Administrador de base de datos.

Asimismo, cuando así se precise, y en todo caso, cuando se acceda a ficheros que contengan datos de carácter personal a los que se asignen nivel medio o alto de seguridad, se requerirá la introducción de una palabra de paso adicional, específica para el sistema de información, con objeto de reforzar las medidas de seguridad en el acceso al mismo.

Decimoséptimo. *Acceso de usuarios externos a la red de informática presupuestaria.*—El acceso de usuarios ajenos a la red de informática presupuestaria, en los términos señalados en esta Resolución, a los sistemas de información de la Secretaría de Estado de Presupuestos y Gastos se ajustará a los criterios anteriormente expuestos con las adaptaciones que se indican a continuación.

Con carácter general, estos usuarios, sin perjuicio de lo que se establece en el apartado siguiente, cuando sean autorizados para acceder a bases de datos de la Secretaría de Estado de Presupuestos y Gastos no precisarán que sus estaciones de trabajo estén configuradas bajo el procedimiento técnico de integración de sistemas de los servicios de informática presupuestaria (ISIP).

La solicitud de acceso a la base de datos requerida será dirigida por el responsable jerárquico del usuario o de la unidad administrativa en la que va a prestar sus servicios, con categoría mínima de Subdirector general o asimilado, al responsable del centro al que corresponda la administración funcional de la base de datos. En el caso de autorizar el acceso solicitado, el responsable de centro comunicará dicha autorización y los términos de la misma al correspondiente Administrador de base de datos, quien, con carácter previo a su instrumentación, la comunicará a la unidad designada de los servicios de informática presupuestaria quién coordinará con el Administrador de base de datos anteriormente indicado la operatividad del acceso concedido.

En la solicitud de acceso dirigida al responsable de centro se indicará el usuario o usuarios para los que se propone el acceso, el sistema de información a acceder, el perfil de acceso requerido, una justificación debidamente fundamentada, la ubicación y una persona de contacto, con su teléfono y dirección de correo electrónico. Asimismo, se hará constar la fecha propuesta para el alta y la fecha de caducidad para dicho acceso.

El identificativo lógico de usuario asignado a un usuario externo tendrá una vigencia máxima de doce meses, debiendo ser expresamente renovado una vez transcurrido dicho periodo, a instancia del órgano en que preste servicio el usuario.

Los usuarios externos que fueran autorizados a acceder a sistemas de información de la Secretaría de Estado de Presupuestos y Gastos se dotarán a sí mismos con medios técnicos y cumplimentarán y respetarán los procedimientos establecidos en esta Resolución.

En caso de incumplimiento de esta normativa sobre accesos, el Administrador de base de datos podrá proponer la revocación de las autorizaciones concedidas a las que se refiere este apartado.

Decimooctavo. *Acceso a bases de datos externas.*—Cuando la base de datos a la que se desea acceder resida fuera del entorno de la red corporativa de informática presupuestaria (base de datos de la AEAT; de la Seguridad Social, ...), facilitándose a través de dicha red la conexión a la base de datos externa, sin perjuicio de observar los requerimientos de seguridad y control de accesos específicos del dominio externo al que se accede, actuará como Administrador de acceso a dicha base de datos, a efectos de esta Resolución, la persona que designe el Coordinador de los servicios de informática presupuestaria.

Decimonoveno. *Notificación y gestión de las incidencias.*—Los Administradores de red y de base de datos comunicarán inmediatamente al responsable de seguridad cualquier anomalía o irregularidad detectados en los mecanismos adoptados para garantizar la seguridad en el control de accesos, a través del sistema de información establecido para la notificación y gestión de incidencias.

Todas las anomalías o irregularidades detectadas en el control de accesos se considerarán «incidentes de seguridad», por tanto:

- a) Se registrará la incidencia en el buzón del Administrador corporativo de seguridad creado para tal efecto.
- b) El Administrador corporativo de seguridad generará correo de notificación de la incidencia detectada en el control de accesos, dirigido al responsable del centro directivo u organización delegada o territorial del

cual depende el Administrador de red o base de datos que detectara la incidencia en cualquiera de los mecanismos adoptados para garantizar la seguridad en el control de accesos.

c) El Administrador corporativo de seguridad realizará un seguimiento exhaustivo de la incidencia hasta su resolución.

d) Tras la resolución de la incidencia se procederá al cierre de la misma por el Administrador corporativo de seguridad. La incidencia pasará a formar parte del registro histórico de incidencias de seguridad.

e) El Administrador corporativo de seguridad generará correos de notificación de cierre de la incidencia, dirigidos al Administrador de red o base de datos que detectara la incidencia en cualquiera de los mecanismos adoptados para garantizar la seguridad en el control de accesos y al responsable del centro directivo u organización delegada o territorial del cual dependa.

Vigésimo. *Auditoría del procedimiento de control de accesos.*—El Administrador corporativo de seguridad promoverá la realización de auditorías sobre la aplicación del procedimiento de control de accesos y acerca del propio procedimiento, al menos, cada dos años.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (Real Decreto 994/1999), identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

La auditoría verificará cada uno de los ficheros de datos de carácter personal, soportados dentro de la red de informática presupuestaria, a los que correspondan la aplicación de medidas de seguridad de niveles medio o alto.

Vigésimo primero. *Confidencialidad de la información.*—Los datos e informaciones contenidas en las bases de datos de la Secretaría de Estado de Presupuestos y Gastos, cualquiera que sea su soporte, serán de uso exclusivamente reservado para el cumplimiento de los fines que le atribuye el ordenamiento jurídico.

Las autoridades, funcionarios públicos y demás personal al que resulte de aplicación esta Resolución y que por razón de su cargo o función tuviesen conocimiento de los datos o informaciones a que se refiere el párrafo anterior, están obligados a guardar sigilo riguroso y observar estricto secreto respecto de los mismos.

El personal autorizado sólo deberá acceder a las bases de datos cuando deba conocer determinada información por razones del servicio, debiendo abstenerse de hacerlo por cualquier otra motivación.

La salida de soportes informáticos que contengan información de las bases de datos de la Secretaría de Estado de Presupuestos y Gastos, únicamente podrá ser autorizada por el responsable de centro.

Vigésimo segundo. *Responsabilidades.*

a) Cada usuario deberá conocer y aplicar, en su ámbito de actuación, la presente Resolución, así como las normas, instrucciones y procedimientos que en materia de control de accesos a la red y bases de datos de la Secretaría de Estado de Presupuestos y Gastos se establezcan.

b) Cada usuario, debidamente autorizado, adquiere el compromiso de utilización de las bases de datos con los fines exclusivos de gestión para los que ha sido autorizado. Asimismo, será responsable de todos los accesos que se realicen mediante el uso de su código de identificación lógica de usuario y su correspondiente palabra de identificación personal. A tal fin deberá mantener la custodia y secreto de la indicada PIP, así como vigilar posibles usos ajenos, denunciando cualquier transgresión.

En ningún caso deberá facilitarse el código de usuario ni la palabra de identificación personal a otras personas, ni deberá accederse a las bases de datos utilizando códigos y PIP ajenos, incluso mediando el consentimiento del usuario titular.

c) El cese de un usuario en el puesto de trabajo por cualquier causa determinará el cese automático como usuario, a cuyo efecto, tan pronto como se produzca el cese en el puesto, el responsable jerárquico superior que, en el caso de servicios centrales, tendrá categoría mínima de Subdirector general o asimilado, y, en el supuesto de tratarse de organizaciones delegadas o territoriales, será el máximo responsable de la organización, lo comunicará al Administrador de la red y, a través de éste, a los Administradores de base de datos que corresponda según su perfil.

Cuando se trate de un usuario externo al ámbito de la Secretaría de Estado de Presupuestos y Gastos, su cese será comunicado, por el responsable jerárquico que efectuó la solicitud, al Administrador de base de datos, quien coordinará con la unidad designada de los servicios de informática presupuestaria la instrumentación de la baja correspondiente.

d) El acceso a la información de las bases de datos de la Secretaría de Estado de Presupuestos y Gastos por un usuario no autorizado, la realización de transacciones informáticas que no estén relacionadas con un objetivo concreto de gestión, la asignación de perfiles de utilización

a otras personas para el uso de transacciones no necesarias para la gestión que tengan encomendada, o la revelación o falta de diligencia en la custodia y secreto de su código de usuario y palabra de identificación personal darán lugar a la exigencia de las responsabilidades administrativas o de otra naturaleza en que se hubiese podido incurrir.

En el supuesto en que las actuaciones señaladas en el párrafo anterior hubiesen sido cometidas por un funcionario público, las mismas podrán dar lugar a la incoación del oportuno expediente disciplinario a tenor de lo previsto en los artículos 6, 7 y 8 del Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado, aprobado por Real Decreto 33/1986, de 10 de enero.

De igual modo, las conductas señaladas en los párrafos anteriores darán lugar a la supresión de las autorizaciones previamente concedidas por quien las hubiera otorgado en su momento.

Vigésimo tercero. *Medios.*—Los servicios de informática presupuestaria de la Intervención General de la Administración del Estado establecerán, en el ámbito de la Secretaría de Estado de Presupuestos y Gastos, los procedimientos, aplicaciones, programas, utilidades y medios necesarios para facilitar el cumplimiento de la presente Resolución.

Vigésimo cuarto. *Período de adaptación.*—La adaptación de los procedimientos, aplicaciones, programas, utilidades y medios a lo dispuesto en esta Resolución se llevará a cabo en el período de doce meses desde la entrada en vigor de la misma.

La designación de los Administradores de red y de base de datos, se efectuará en el plazo de dos meses desde la entrada en vigor de la misma.

La confirmación, en su caso, de las autorizaciones, actualmente operativas, de acceso a la red y a las bases de datos se efectuará en el plazo de cinco meses desde la entrada en vigor de la misma.

Vigésimo quinto. *Aplicación a la Dirección General de Fondos Comunitarios y Financiación Territorial.*—La Dirección General de Fondos Comunitarios y Financiación Territorial adaptará el contenido de esta Resolución para los sistemas de información y bases de datos del área de financiación territorial cuya gestión informática asume directamente.

Vigésimo sexto. *Desarrollo para su aplicación.*—Se faculta a la Intervención General de la Administración del Estado para resolver cuantas consultas de índole específica puedan plantearse en la aplicación de la presente Resolución, así como para dictar normas internas para su aplicación.

Vigésimo séptimo. *Entrada en vigor.*—La presente Resolución entrará en vigor el día siguiente de su publicación en el «Boletín Oficial del Estado».

Madrid, 8 de julio de 2002.—La Secretaria de Estado, María Elvira Rodríguez Herrero.

MINISTERIO DE FOMENTO

14811 *RESOLUCIÓN de 28 de junio de 2002, de la Dirección General de la Marina Mercante, por la que se declara la homologación del equipo Radioteléfono de VHF No-Solas, marca «Sailor» modelo RT-2048, para su uso en buques y embarcaciones de bandera española.*

Visto el expediente incoado a instancia de la empresa «Nautical, Luis Arbulu, Sociedad Limitada», con domicilio en calle Gomera, 8, 28700-San Sebastián de los Reyes-Madrid, solicitando la homologación del equipo Radioteléfono de VHF No-Solas, marca «Sailor» modelo RT-2048, para su uso en buques y embarcaciones de bandera española y de acuerdo con las normas:

Real Decreto 1890/2000 de 20 de noviembre. Resolución de 23 de marzo de 2001 de la SETSI. Reglamento de Radiocomunicaciones.

Esta Dirección General ha resuelto declarar homologado el siguiente equipo radioeléctrico:

Equipo: Radioteléfono de VHF No-Solas. Marca/modelo: «Sailor»/RT-2048. Número homologación: 50.048.

La presente homologación es válida hasta el 27 de junio de 2007.

Madrid, 28 de junio de 2002.—El Director general, José Luis López-Sors González.